SIBIRI INNOVATION (OPC) PVT LTD
Corporate Architecture · Standards · Engineering Documentation

DOC REF: SBR-SEC-005
VERSION: 4.0.0
RELEASE DATE: September 26, 2026

CYBERSECURITY & COMPLIANCE VERIFIED STANDARD

Enterprise Cyber Defense & OWASP Top 10 Hardening Guide

SQLi, XSS, CSRF Mitigation, Secure Headers & CSP Directives

Document Scope:	Baseline security requirements for all production web applications and APIs.
Target Audience:	Security Auditors, Compliance Officers, Full-Stack Developers
Classification:	Public · Royalty-Free Engineering Reference · ISO/IEC Aligned

1. EXECUTIVE SUMMARY & STANDARDS ALIGNMENT

Comprehensive enterprise application hardening manual addressing each vulnerability in the OWASP Top 10. Details parameterized query enforcement, strict CSP header policies, SameSite cookie configurations, and dependency vulnerability scanning in CI/CD.

2. DEFENSE-IN-DEPTH SECURITY MATRIX

Sibiri applications implement defense-in-depth across the network, application runtime, and database layers.

- Content-Security-Policy (CSP) with cryptographic nonces preventing unauthorized inline scripts.
- Strict HTTP Strict Transport Security (HSTS) with 2-year max-age and preload directives.
- Automated SAST/DAST scanning on every code commit prior to production deployment.

INSTITUTIONAL GOVERNANCE & ENGINEERING SLA

This document represents the official architectural baseline maintained by SIBIRI INNOVATION (OPC) PVT LTD. All client deliveries, source code handovers, and academic installations adhere strictly to the protocols outlined herein.